# What Privacy and Confidentiality Mechanisms are used in the Electronic Health Records (Clinical Master and ICT4 M-Power systems)? A design Science Research Approach.

Glorious Orishaba[a,*], David Serunjogi[b]

[a] *Department of Epidemiology and Biostatistics, School of Public Health, Makerere University, Uganda*
[b] *Medical Research Council /Uganda Virus Research Institute and London School of Hygiene and Tropical Medicine Uganda Research Unit.*

**Abstract**

**Background:**

Patients are required to share information with their doctors to facilitate correct diagnosis and determination of treatment, especially to avoid adverse drug interactions. Despite efforts to fully implement and adopt Electronic Health Records System, there is limited attention to fully secure patients' details. Issues of privacy and confidentiality still remain a major concern at health facilities mainly in developing countries like Uganda. This study aimed to determine what privacy and confidentiality mechanisms are used in the EHRs (Clinical Master and ICT4 M-Power systems

**Methods**:

The study used a design science research approach that adopted qualitative methods. Data Flow Diagrams were used to design the desired artefact while the development of the encryption and decryption tool, we used the Hypertext Pre-Processor(PHP) time platform, which is an object-oriented programming language and is a block component that is made up of Cascade Style Sheet (CSS) and HTML(hypertext markup language ) embedded in PHP for it to be fully functional and be able to connect to and run on the server where most of the records and details of the activities are stored in the database.

**Results:**

The respondents pointed at various current mechanisms for privacy and confidentiality that included; user credentials, segregation of roles, Physical access control, international access policies, interlocked interface screens, and training of users.

**Conclusion:**

The inclusion of encryption and decryption features are very vital to enhancing health facilities' capacity and measures for establishing the privacy and confidentiality of patients' data.

**Recommendation:**

The Ministry of Health, Uganda, and implementers of EHR should adopt the encryption and decryption tool for use at the health facilities as the second layer of security to ensure the privacy and confidentiality of patients' data.

*Keywords:* Privacy, Confidentiality Mechanisms, Electronic Health Records, Date Submitted: 2022-07-10 Date Accepted: 2022-08-26

## 1. Background of the study

Privacy is described as the ability to determine for people when, how, and to what extent information about people is communicated to others. Parrott, Burgoon, and LePoire (2003) identified four types of privacy: physical privacy, social privacy, psychological privacy, and informational privacy. Informational privacy refers to having control over external access to personal information and protection against the disclosure of such information.

Confidentiality involves a set of rules or a promise usually executed through confidentiality agreements that limit access or place restrictions on certain types of information. Confidentiality is closely related in meaning to one of the major uses of the term "privacy," namely, informational privacy. In health care interactions, patients communicate sensitive personal information to their caregivers so that the caregivers can understand patients' medical problems and treat them appropriately. By calling such information confidential, we indicate that those who receive the information have a duty to protect it from disclosure to others who have no right to the information (Moskop,2005).

Patients are required to share information with their doctors to facilitate correct diagnosis and determination of treatment, especially to avoid adverse drug interactions (Jimmy & Jose, 2011). However, most patients may refuse to divulge important information in cases of health problems such as psychiatric behavior and HIV status as their disclosure may lead to social stigma and discrimination. Over time, patient health records can serve a range of purposes apart from diagnosis and treatment providers as patients ' medical records accumulate significant personal information including identification, history of medical diagnosis, digital renderings of medical images, and treatment received among others (Tesema, Medlin, & Abraham, 2010). With the importance of patients' medical records, which are shared with payer organizations such as insurance, Medicare, or Medicaid to justify payment of services rendered by physicians, healthcare providers may use records to manage their operations, assess service quality, and identify quality improvement opportunities (Essay Sauce, 2012). The motives for compromising privacy and confidentiality of patients' information could be either economic or non-economic nature. For instance, some individuals such as insurers, employers, and journalists take and utilize patients' records for economic gains, while others may have noneconomic motives such as a person involved in a romantic relationship. These attackers may have resources ranging from modest financial backing and computing skills to a well-funded infrastructure to threaten a patient as well as the operations of a healthcare facility. In addition, threats could depend on the technical capability of attackers who may be novice or sophisticated programmers and thus, easily access (hack into) electronic health records systems. Moreover, with the growing underground cyber economy (Knapp, Ford, Marshall, & Rainer, 2007) notes that an individual with the intent to acquire data and possess adequate financial resources may choose to buy the services of sophisticated hackers to breach healthcare data.

Therefore, the interoperation of EHRs is critical in order to maintain privacy, and access controls. But security measures must be implemented throughout the workflow right from the design and implementation. Unlike traditional paper medical records, EHR systems can be programmed to include encrypted information, audit functions, and other safeguards to maintain the security of health records (Kruse, Smith, Vanderlinden, & Nealand, 2017). No form of electronic security, however, can prevent individuals who view the exchanged data from improperly revealing sensitive information (Hazin, 2013). There have been breaches of privacy and confidentiality related to patients' information in healthcare facilities and particularly in health and non-healthcare providers' offices with the existence of limited yet violated measures for ensuring privacy and confidentiality of patient

*Corresponding author.
*Email address:* gorishaba@gmail.com (Glorious Orishaba)

data (Beltran-Aroca, GirelaLopez, Collazo-Chao, Montero-Pérez-Barquero, & Muñoz-Villanueva, 2016). This study focused on the development of the encryption and decryption tool for the privacy and confidentiality of patients' information stored in the EHR system at the health facility.

## 2. Methodology

**Study design:**

The Design Science Research approach was used during the creation of a practical solution to solve an identified problem which is in line with the study aim. The model always begins with problem identification and motivation while the objectives of a solution are adaptively drawn using existing knowledge. Then, an artefact that solves the problem is designed and developed. The implemented artefact is demonstrated, evaluated, and communicated.

**Setting:**

The study was conducted at 2 study sites; a public and private health facility at Mukono Health Center IV (now Mukono General Hospital) and Doctors Medical Center – Kampala respectively. These two healthcare facilities were selected in order for the researcher to understand the perspectives of what is in private and public health facilities in relation to EHRs because they both have EHRs that are used at the point of care. Notably, Mukono Health Center IV is a public health facility that provided real lived experiences of EHRs since it uses ICT4 M-Power while Doctors' Medical Center – Kampala provides perspectives of private health facilities as it uses Clinical Master as the EHR system. In terms of patients' capacity, Mukono health center IV has high a volume facility compared to doctors' medical center. With regards to system capacity, this may largely depend on the number of users who computer the data. Mukono Health Centre IV commonly known as Mukono Mini Hospital is an outpatient health facility located on the Kampala-Jinja Highway, in Mukono Municipality, approximately 20 kilometers (12 miles), east of Kampala, the capital and largest city in the country. While, Doctors' Medical Center – Kampala is a private facility located at Mpererwe along Kampala Gayaza Road, it's a health maintenance organization (HMO) that provides affordable healthcare insurance to its clients. Data were collected between February and March 2021 and a total of fifteen (15) respondents were interviewed.

**Participants:**

The study population comprised healthcare workers (Medical Officers, Nurses, Midwives, Lab Technicians, and Pharmacist) and support staff (Accountants, Health Information Officers, and IT Technicians), and hospital management (administrators, in-charge and head of sections). The facility staff who interacted with the electronic health records systems (ICT4 M-Power and Clinical Master) at Mukono General Hospital and Doctors' Medical Center – Kampala were involved in the study. Nonetheless, any facility staff at Mukono General Hospital and Doctors' Medical Center – Kampala that did not interact with the electronic health records systems (ICT4 M-Power and Clinical Master) and those that ever used the system but are no longer staff at the facilities were excluded.

In this study, a non-probability of sampling (purposive sampling) was used to select respondents from each study site based on the characteristics of the population, the objective of the study, and the responsibility they had to the electronic health records systems.

Notably, from Mukono Health Center IV (which uses the ICT4 M-Power system).

**Data sources:**

A data collection tool was developed by the researcher based on insights gained through the literature review. The interview tool was reviewed by a senior Health Informatician and researcher in the field, and edited by the principal investigator/researcher based on feedback. The interview questions were reviewed and modified by consensus between the principal researcher and research assistant who had vast knowledge of the Health information system and the healthcare system of Uganda. The interview study tool used for this study is presented in Appendix II of this document.

Each interview was treated as an individual

case, and interviews were audio-recorded and de-identified. In cases where the interviewee wasn't comfortable with audio recording, the researcher took shorthand notes which were later expanded. Throughout the process of the interviews, probes and follow-up questions were added as needed to encourage amplification and elucidate responses. Specific questions were added as the interview process proceeded and data collection was terminated when the researcher realized that the respondents were no longer mentioning any new information in regard to the security concerns in the system (reached point of saturation). The secondary data collection approach used in this study was a document review of the existing EHR user manuals for ICT4 M-Power and Clinical Master and also policy analysis was performed (for instance HIPAA 2013, Computer Misuse Act 2011 among others) to supplement the primary approach used to answer ROs 1 & 2. This helped the researcher to triangulate data got from other sources and deepen the knowledge of existing EHR systems and practices and therefore facilitating the successful implementation of the encryption and decryption tool.

### Study size

A total of 10 key informants were sampled and interviewed this is because it had a fairly bigger number of users (28) and thus, 10 key informants were considered a fair representation as the researcher realized no new information was coming from the 10th respondent. Similarly, from Doctors' Medical Center – Kampala (that uses Clinical Master) a total of 5 key informants were sampled and interviewed. The facility has a smaller staff population and patient turnover compared to Mukono General Hospital, thus, out of 15 users of the Clinical Master system, 5 staff were considered a fair representation of the entire population and interviewed. The key informants were consciously and purposively picked across the different departments, units, and sections of the facility to have a true representation of all staff that interacts with the systems.

## 3. Results

### Description of the Current Privacy and Confidentiality Measures

#### User Credentials

Results indicated users for the EHRs; Clinic Master and ICT4 M-Power have been assigned user credentials in form of user names and passwords to access the system. Users are categorized depending on the department or unit they belong to, such as reception, pharmacy, laboratory, maternity, and accounts among others. Thus, users are able to only access those services as offered in the different departments. However, because there is a limited number of computers at the health facilities, it so happens that the majority of users tend to share the computers. In addition, because the staff (personnel) at the health facility are few, when one doesn't report for work, it will so happen they will share with the colleague their username and password. This eventually creates a threat to patients' data due to loss and misuse of user credentials.

#### Segregation of Roles

The roles of system users in ICT4 M-Power and Clinical Master have been clearly segregated. For instance, the clinician has a dashboard to capture information related to clients' illness history and condition, prescriptions, and recommendations including referring for laboratory diagnosis. At the Lab level, the Lab Technician is only able to see the lab requests from the clinicians. After, the test results are fed into the system and sent back to a clinician who does the prescription. Once the Clinician has fully diagnosed and prescribed treatment to the patient, there is not any other way the information can be seen by other users.

At this stage, the patient is referred to the pharmacy or dispensing unit with an electronic prescription note. Lastly, at the pharmacy (dispensing unit), data from the clinician is retrieved to aid dispensing. The data about actual drugs and supplies dispensed is fed into the system including payments made. At every stage, a particular user can only access and view what they are meant to see with regards to a particular service or care to

a given patient, as indicated in the quote below:

*We hold our patients' data as very sensitive and vital at every point of care within our health facility; you can't just see their data, no.., if you do not have a personal username and password there is no way you can get it even if the patient seeking care is a relative to you as a staff* – **Receptionist, Doctors' Medical Center - Kampala.**

**Interlocked Interface Screens**

According to the ICT4M-Power system, every module has its page and every page has a person who is authorized to open and access the data, as was asserted by a Clinician from Mukono Health Center IV that;

*This system is made in a way that each of the users has a username and password with a dashboard that has specific roles for each user; say a clinician like me so you only write and feed what you have to in your page and afterward send to another point of care like to the Lab* - **Clinician, Doctors' Medical Center - Kampala .**

**Training of Users**

Before implementation of the system, every system user is trained to ensure security and effective use of the system. The issues covered include the functionality of the system and majorly how to maintain the privacy and confidentiality of patients' data.

In addition to training is the fact that the system has colours that are assigned to indicate the current health condition of patients whose meaning is known and only interpreted by health workers or systems that are involved in using the system. The assignment of colors is done to ensure confidentiality of the patient's health conditions and related information as illustrated by a Medical Records Officer;

*The system has manual color codes; blue, yellow, and red that the guys who came from Sweden put. We have different colors in the system that we use to indicate patients' health conditions or state of illness which anyone else may not know. When the person comes and is not in good condition, for example, we have yellow, which is assigned to slightly sick patients or a bit seriously sick. We have read, for someone who is seriously ill and once I assign someone red color automatically goes on top of others for the doctor to pick this patient for faster service delivery* – **Medical Records Officer, Mukono Health Centre IV.**

Therefore, results related to training of systems users indicated that just a few of the health facility personnel received orientation on how to use and thorough training about functionality of either clinical mater or ICT4 M-Power.

**Physical Access Control**

Results indicated that both ICT4 M-Power and Clinical Master systems had privacy measures in place for ensuring the privacy and confidentiality of patient data, which includes; physical access control for authentication checks, for example, burglar-proof doors with biometrics.

On the other hand, computers are fully guarded against any threats and viruses. Firewalls are fully installed and the anti-virus is routinely updated for checking and detecting any threats. Automatic backups have also been automated to avoid any loss of data. This has been illustrated in the quotation below as;

*Security being that it's very important in regards to keeping patients' data, our health facility placed measures in place such as; firewalls and anti-virus soft-wares that are updated now and then to ensure that they work effectively. In addition, we have backups and physical access control to ensure that access to patient's data is not for every Tom, Dick, and Harry. These security measures have helped our facility not face any legal liabilities that could arise as a result of information leaks* – **Medical Records Officer, Mukono Health Centre IV.**

Study findings related to privacy measures indicated that just a few have been so far integrated at the facility included; authentication checks and most importantly physical access controls which have strengthened the privacy of client information and built trust and efficiency.

**Internal Access Policies**

At the different health facilities respondents indicated that they have introduced internal access policies to guide use of the EHR implemented. This has been affirmed by the quote below;

*We have our physical internal policies for ex-*

*ample not sharing passwords with other people, you must make sure the password is only yours and in case you realize that someone stealthily accessed your password or known the password so we are always advised to change it immediately and most times we are advised to change passwords every after three months just to make sure that your password is safe and no one can access it* – **Clinician, Doctors' Medical Centre – Kampala.**

**Data Management and Analysis**

At the end of the interview process, the audio recordings were transcribed verbatim by the researcher and validated independently by a research assistant with knowledge in health informatics who re-listened to the audio recordings to ensure they were accurately transcribed. Observations from the research assistant were shared with the researcher who incorporated them into the final interview script. Both the researcher and the research assistant engaged in a reflexive dialogue to conduct an open inductive analysis. Open Inductive analysis, is an approach to data analysis that aims at deriving more general concepts through the interpretation of raw textual data (Braun, 2006; Krippendorff, 2004). After the initial analysis of data, the researcher shared the preliminary results of the study with the respondents (in consultative discussion) to ascertain if what they shared was well presented and get their views about the encryption and decryption tool developed.

The feedback from this consultative discussion was used and informed the refinement of the tool after familiarization with the raw data a coding scheme was developed in a multi-level process. Statements that mentioned mechanisms, challenges, requirements, features, and recommendations were identified and categorized into codes. Any discrepancies were discussed and new codes or code definitions were created. The truthfulness of findings was enhanced through frequent discussion between the researcher, and research assistants to ensure that the codes, subthemes, and themes adequately described and encompassed the data collected. While the responses from the observation checklist were analyzed and presented as proportions based on respondents.

## 4. Discussion

**Privacy and Confidentiality Mechanisms Used in EHR and Challenges Faced**

This study aimed at developing an encryption and decryption tool for the privacy and confidentiality of patients' data in the EHRs. The use of encryption and decryption tools provides a second layer of security for patients' data in the EHR, the testing of the functionality of the tool showed that data is encrypted at the source and can only be decrypted by the recipient who has received the decryption key. Like most of the health records systems in Uganda, ICT4M-Power and Clinical Master have a core function mainly login accounts and passwords for purposes of interacting with these systems to purposely access the patients' data and ensure the privacy and confidentiality of patients' records. The presence of a role definition and a page for every user of the systems with its defined access rights is aimed at ensuring the privacy and security of patients' data as per the requirements of the Uganda E-Health Misuse Act 2011 and Data Protection Act 2011.

It was evident that the ICT4M-Power system satisfies both local and international standards and regulations which make it a generally acceptable system. The standards and regulations include; HIPPA, HMIS guidelines, the Uganda E-Health Misuse Act 2011, Data Protection Act 2011, and the Computer Misuse Act as well as ISO Lab certification. However, the system conforms to and satisfies just sections of privacy and confidentiality requirements in these standards and regulations leaving a lot to be desired. The clinical Master system satisfies four standards such as HIPPA, the Uganda E-Health Misuse Act 2011, Data Protection Act 2011, and the Computer Misuse Act 2011. However, the absence of different layers of security and data encryption stand as critical standards that needed to be met for the system to ensure the privacy and confidentiality of patients' data.

## 5. Conclusion:

The inclusion of encryption and decryption features are very vital to enhancing health facilities' capacity and measures for establishing the privacy and confidentiality of patients' data.

**Recommendation:**

The Ministry of Health, Uganda, and implementers of EHR should adopt the encryption and decryption tool for use at the health facilities as the second layer of security to ensure the privacy and confidentiality of patients' data.


## Acknowledgment

I thank the Almighty God for bringing me this far, it has always been his love and Mercy. I also thank my family and friends for the support accorded to me throughout the course, thank you so much you have been a great pillar to my course. I express my heartfelt gratitude to HITRAIN Project for funding this research – with your generous financial support, I have been able to complete the research with ease. My sincere thanks to my Supervisors Prof. David Guwatudde and Dr. Kahiigi Evelyn for the untiring scholarly guidance and support given to me during this research.

I also express my appreciation to research participants from Mukono Health Center IV (Mukono General Hospital), and Doctors Medical Center - Kampala. My special thanks also go to my coursemates especially Anibare Niwamanya, Muwanguzi Samuel, and James Sserubungo for the support given to me during the course.


**List of Abbreviations.**

CAMRA: Confidential Audits of Medical Record Access

EHR :Electronic Health Records

HF: Health facilities

HIPAA: Health Insurance Portability and Accountability Act

HMIS: Health Management Information System

ICT: Information Communication Technology

ICT4 M-Power: Information Communication Technology Powering Medical

MOH: Ministry of Health

PRIMA: Privacy Management Architecture

RBAC: Role-Based Access Control

UDHS: Uganda Demographic Health Indicator Survey.

WHO : World Health Organization


**Source of funding.**

This study was not funded.


**Conflict of interest**

No conflict of interest declared.

## Appendix A. References:


1) Catherine A.MarcoMDGregory LukeLarkinMD, MSPHJoel M.GeidermanMDArthur R.DerseMD, JD (2005) From Hippocrates to HIPAA: Privacy and confidentiality in Emergency Medicine-Part I: Conceptual, moral, and legal foundations

2) Coulentianos M, Rodriguez-Calero I, Daly S, & Sienko K (2020).Global health front-end medical device design: The use of prototypes to engage stakeholders. Journal of development engineering vol. 5(2020) 100055.https://doi.org/10.1016/j.deveng.2020.100055

3) Essay Sauce, Information Security And Privacy In Healthcare Management System. Available from:<https://www.essaysauce.com/business-essays/information-security-privacy-healthcare/> [Accessed 23-07-22].

4) Hazin, R., Brothers, K. B., Malin, B. A., Koenig, B. A., Sanderson, S. C., Rothstein, M. A., Williams, M. S., Clayton, E. W., & Kullo, I. J. (2013). Ethical, legal, and social implications of incorporating genomic information into electronic health records. Genetics in medicine : official journal of the American College of Medical Genetics, 15(10), 810-816. https://doi.org/10.1038/gim.2013.117

5) Jimmy, B., & Jose, J. (2011). Patient medication adherence: measures in daily practice. Oman medical journal, 26(3), 155-159. doi:10.5001/omj.2011.38https://doi.org/10.5001/omj.2011.38

6) Khan, N., Yaqoob, I., Hashem, I. A. T., Inayat, Z., Mahmoud Ali, W. K., Alam, M., Gani, A. (2014). Big Data: Survey, Technologies, Op-

portunities, and Challenges. Thehttps://doi.org/10.1155/2014/712826

7) Knapp, K. J., Ford, F. N., Marshall, T. E., & Rainer, R. (2007). The common body of knowledge: A framework to promote relevant information security research. Journal of Digital Forensics, Security and Law, 2(1), 1.https://doi.org/10.15394/jdfsl.2007.1016

8) Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. Journal of medical systems, 41(8), 127-127. doi:10.1007/s10916-017-0778-4https://doi.org/10.1007/s10916-017-0778-4

9) MOH (2017). Uganda National e-Health Strategy 2017 -2021. Ministry of Health, Kampala, Uganda.

10) Moskop, J. C., Marco, C. A., Larkin, G. L., Geiderman, J. M., & Derse, A. R. (2005). From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine–Part I: conceptual, moral, and legal foundations. Annals of emergency medicine, 45(1), 53-59. https://doi.org/10.1016/j.annemergmed.2004.08.008

11) Neal, D. (2011). Choosing an electronic health records system: professional liability considerations. Innovations in clinical neuroscience, 8(6), 43-45.

12) Phillips, W. (2015). Ethical controversies about proper health informatics practices. Missouri medicine, 112(1), 53-57.

13) SenaySarmasogluPhD, RNaLeylaDincPhD, RNbMelihElcinMD, MSc, CHSEcGul HaticeTarakcioglu CelikMSN, RNaIslePolonkoGTAd (2016) Success of the First Gynecological Teaching Associate Program in Turkeyhttps://doi.org/10.1016/j.ecns.2016.03.003

14) Tesema, T., Medlin, D., & Abraham, A. (2010). Patient's perception of health information security: The case of selected public and private hospitals in Addis Ababa. Paper presented at the Information Assurance and Security (IAS), 2010 Sixth International Conference on.https://doi.org/10.1109/ISIAS.2010.5604053

## Appendix B. Publisher details:

**Publisher: Student's Journal of Health Research (SJHR)**
**(ISSN 2709-9997) Online**
**Category: Non-Governmental & Non-profit Organization**
**Email: studentsjournal2020@gmail.com**
**WhatsApp: +256775434261**
**Location: Wisdom Centre, P.O.BOX. 148, Uganda, East Africa.**